



WHITEPAPER

# The Power of Next- Generation SD-WAN: Delivering an Unmatched User Experience with App- Defined Fabric

Application-aware SD-WAN is the key to enhancing network performance, offering a comprehensive solution that identifies application signatures, steers traffic, and optimizes performance. Discover how application awareness can improve user experience and transform network management in the future.

## Introduction

Life is all about performance, whether it's compiling a high batting average, playing concert piano before an audience, or managing an enterprise IT network system upon which multitudes of people rely daily.

Excellent performance in IT networking is all about internet service providers obtaining outstanding speed and uptime metrics from their trusted tech partners to provide airtight service-level agreements (SLAs) on a 24/7 basis. These contracts between ISPs and their customers define the level of service that the ISP will provide.

Here are some of the specific ways that ISPs use SLAs to ensure quality networking:



**Uptime:** ISPs typically guarantee a certain level of uptime, such as 99.9%. This means that the network should be available for use 99.9% of the time. If the network is down for more than 0.1% of the time, the ISP may be liable to pay the customer a penalty.



**Response time:** ISPs also typically guarantee a certain level of response time, such as 15 minutes. This means that the ISP should respond to customer requests for help within 15 minutes. If the ISP takes longer than 15 minutes to respond, the customer may be able to claim a refund or discount.



**Bandwidth:** ISPs typically guarantee a certain amount of bandwidth, such as 100 Mbps. This means that the customer should be able to download and upload data at a speed of 100 Mbps. If the ISP cannot provide the customer with the guaranteed bandwidth, the customer may be able to claim a refund or discount.

By including these metrics in their SLAs, ISPs can ensure that they are providing their customers with a high-quality networking experience.

So how does an enterprise optimize its application performance to be as intelligent, swift and secure as possible? Read on.

## What is Application Awareness, and Why is it Important?

Simply put, application awareness is accurate application intelligence that understands applications of all kinds — business critical, SaaS, internet and cloud. This is an important functionality that is required in any solution that connects, manages and secures users to applications. It's the kind of functionality you don't often see as part of an SD-WAN solution because it's a large step ahead of where legacy systems are today.

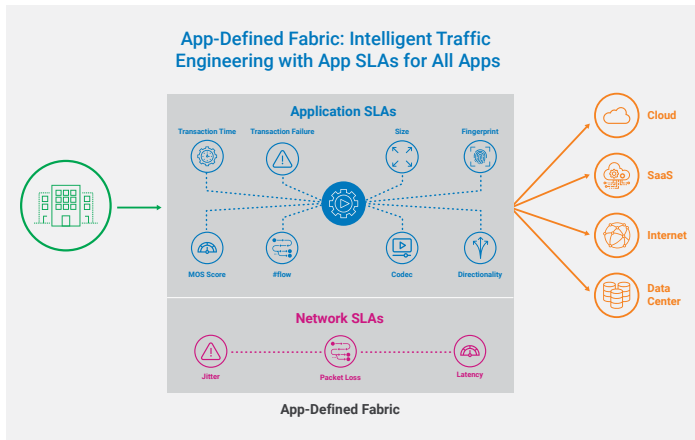
Many network administrators claim that their networks can detect the applications being used. However, it is important to ensure the accuracy of this information and use it to improve application performance and user experience. By understanding the application at the level of its SLA — the specific goals that define the ideal performance of a given app — and implementing best practices to ensure those SLAs are met, administrators can steer applications towards paths with better bandwidth and performance. All of this is crucial for achieving application awareness within a network solution.

With application awareness in the background, administrators don't have to constantly think about and monitor whether applications are using the most efficient path to their destinations. Best practices are always implemented, although people can step in at any time and change policies or make a "game-time" decision in a particular use case.

## Apps Also Can Unexpectedly Change Behavior During Networking Flow

Apps sometimes throw curve balls during a network interaction; this is another reason application awareness is very important. SaaS, apps and sub-apps can drastically change behavior in the middle of the network flow. For instance:

- **They can use different ports and protocols than the underlying network.** For example, a web application might use port 80 for HTTP traffic, but a SaaS application might use a different port, such as 443 for HTTPS traffic. This can make it difficult for network administrators to track and manage traffic.
- **They can introduce new services and features that can change the way traffic flows through the network.** A SaaS application might provide a chat service that uses a different protocol than the underlying network. This can cause traffic to be routed differently, which can impact performance and security.
- **Today's apps have more than one sub-application.** A SaaS or cloud application typically is a suite of parent and sub-applications. It's more important to understand how these sub-applications are identified and mapped to its parent for any traffic forwarding decision.
- **Classification and identification of encrypted applications.** Most applications are built with encryption that makes it harder to identify and classify as SaaS, UCaaS or cloud apps because they all use SSL to protect the application signature.



## Key Attributes of Application Awareness Inside a Network

Application awareness can improve the performance, security and reliability of networks. By making forwarding decisions based on signatures, application awareness can help to ensure that traffic is routed to the correct application and that malicious traffic is blocked.

High-quality application awareness in a network includes the following:

**Accurate fingerprinting:** Fingerprinting is a technique that identifies applications by their unique characteristics. This can be done by analyzing the application's traffic, such as the headers and payloads of the packets, or by analyzing the application's behavior. Fingerprinting can be used to improve the accuracy of application awareness.

**Differentiating between apps** by examining the following factors:



**Port numbers:** Each application uses a specific set of port numbers. For example, the HTTP protocol uses port 80, while the HTTPS protocol uses port 443. Application awareness can use this information to identify the application that is using a particular port.



**Protocol:** Each application uses a specific protocol. The HTTP protocol is a text-based protocol, for example, while the FTP protocol is a binary protocol.



**Application behavior:** Each application has a unique behavior. For example, the web browser will typically make a series of requests to different web servers, while the email client will typically make a single request to an email server. In addition to these factors, application awareness can also use fingerprinting to identify applications.



**Traffic patterns:** Identifying application sessions with deep understanding of applications and sub-applications is instrumental to any application-aware solution. Similarly, learning SSL traffic patterns to identify which application server they are accessing helps classify between applications with precision.

**Flexibility to define applications** allows network administrators to customize the way that applications are identified and classified. This can be helpful in a variety of situations, such as when new applications are introduced or when existing applications are updated. For example, a network administrator might want to define a new application that is not currently recognized by the network's application-awareness system. To do this, the administrator would need to provide the system with information about the application's traffic characteristics, such as the ports that it uses and the protocols that it employs. Once the application has been defined, the network awareness system will be able to identify and classify traffic for that application.

**Application SLAs** such as transaction time, transaction failures and MOS (Mean Opinion Score) are also important to identifying apps because they can provide clues about the type of application that is being used. For example, a high transaction time may indicate that an application is doing a lot of processing, while a high number of transaction failures may indicate that an application is not working properly. MOS is a measure of the quality of experience (QoE) of a network application and can be used to identify applications that are causing problems for users.

**Prioritizing apps based on parameters**, such as business critical, SaaS or cloud by looking at the following factors:

- **Utilization:** Application awareness can look at the amount of traffic that an application is generating. This can be used to identify applications that are important to the business.
- **Business intent:** It can look at the behavior of an application. For example, applications that are used for critical business functions, such as email or customer relationship management (CRM), are more likely to be business-critical than applications that are used for less important tasks, such as browsing the internet.

Making forwarding decisions based on signatures by comparing the signatures of the traffic to a database of known application signatures. If a match is found, the application-awareness system can then make a forwarding decision based on the application's prior classification. For example, if the traffic is identified as being from a web application, the application-awareness system can forward the traffic to the appropriate web server. If the traffic is identified as being from an email application, the application awareness system can forward the traffic to the email server.

Palo Alto Networks' Prisma SD-WAN delivers on all its required SLAs for networking clients through a number of features and capabilities, which include application awareness, path optimization, a high degree of security, and scalability. Prisma SD-WAN is built to scale the needs of any organization, from small businesses to large enterprises.

## How Does Prisma SD-WAN's App-Defined Fabric Provide Application Awareness?

Gen1 or legacy SD-WAN solutions are packet-based, meaning that they route traffic based on the IP address of the destination. They are top-heavy on routing, requiring a lot of manual configuration to set up and manage. During operations, users must manually configure and manage the SD-WAN devices. By their very nature, this makes Gen1 SD-WAN solutions less efficient and more problematic to manage than newer/Gen2 SD-WAN solutions.

Palo Alto Network's [Prisma SD-WAN](#) solution provides app-defined fabric that is designed around the needs of all applications. This means that the network is configured to optimize performance, security and reliability for the applications that are most important to the business.




An app-defined fabric enables an allowable path (direct Internet, direct MPLS, VPN, satellite, LTE, etc.) for each app, high performance, security and WAN segmentation. Thus, it provides direct-to-app access that ensures an exceptional user experience for all applications, such as SaaS, cloud and business-critical/private applications. Any book-ended solution will enforce a centralized architecture, requiring complex topology and access control changes while creating significant latency.


An important point: The right app-defined solution should provide application availability based on application-performance SLAs, unlike legacy solutions that depend on network SLAs to steer traffic intelligently.

### Specific App-Defined Fabric Features


An app-defined fabric can improve the performance of applications by ensuring that they have the bandwidth they need to function properly, but it also helps improve the security of applications by blocking malicious traffic and isolating applications from each other. It also improves the reliability of applications by providing redundancy and failover capabilities.

Some of the key features of an app-defined fabric include:

- 
**Application awareness:** The network can identify and classify applications. This information can be used to optimize performance, security and reliability for specific applications.
- 
**App-specific policies:** The network can be configured with policies that are specific to each application. This can help to improve performance, security and reliability for each application.
- 
**App-based segmentation:** The network can be segmented based on applications. This can help to isolate applications from each other and prevent problems from spreading.



**App session-based forwarding:** The network can be configured to route traffic for specific applications to specific paths. This can help to improve performance and security for specific applications. Prisma SD-WAN does not spray packets like other solutions, instead takes a session based forwarding that helps distribute and load-balance application traffic in a active-active fashion.



**Granular application monitoring:** The network can be monitored to track the performance and health of specific applications. This information can be used to identify problems with applications and to make changes to improve performance and reliability.

### Prisma SD-WAN's Solution Suite

Prisma SD-WAN has always been built on a top-down architecture. The entire solution is based on what applications are detected in a branch network. Traditional networks typically use routing protocols to identify IP addresses and routes for sending traffic to the connected branches. However, Prisma SD-WAN does not rely on this approach.

What Prisma SD-WAN does is look into an enterprise's branch traffic and validate it in a step-by-step fashion. The platform knows what kind of application(s) are being deployed and offers the flexibility to customize those categories. Once it knows the category and type of the application and such details as version, when it was last patched and whether it's a SaaS, internet or a private app, it will provide default recommendations as well as traffic steering for that app.

Once a user has configured business policies for a particular application, this becomes the data-egress route, and Prisma SD-WAN's traffic engineering takes over from there. It will also check on IP addresses and connectivity but will also recognize if decisions have already been made based on the application signature and the policies.

This is all an amount of detail and control that you don't see every day in the networking world.

## How Prisma SD-WAN Goes Deep Into Networking Requirements

Prisma SD-WAN determines whether a particular network path is in good health before traffic is sent, but it does much more than that. The solution monitors traffic at the application level after it is sent. This allows admins to identify issues that might not be evident from network performance alone, such as a degraded application server on the other end. These issues can cause increased transaction times and failures, which Prisma SD-WAN can track and analyze.

For example, Microsoft Office 365 is being forwarded on a broadband network. The network performance is good, but the application itself is suffering. Prisma SD-WAN will look into the business policies that have been established, provide visibility to them and then immediately look for another viable path. Prisma SD-WAN will then forward it, completely switching the flow to the other available path, also ensuring that network administrators know exactly what's happening.

It's the same scenario if the system needs to locate a different server for the application. The same path can be preserved if the system can reach another server that is performing better. It's just that level of flexibility that Prisma SD-WAN's application awareness capability provides.

All the capabilities Prisma SD-WAN brings result in better overall network performance: faster transaction and app response times, in addition to speedier handling of the processes that compress and decompress large amounts of data – known as codecs – which otherwise can slow down data movement. In the context of real-time applications, codecs are used to ensure that the data is compressed and decompressed quickly enough to be used in real time. This is important for applications such as video conferencing, online gaming and live streaming.

## Elements of Prisma SD-WAN Are All Key to Delivering the Branch of the Future

First identified by IT consulting firm Gartner in 2019 to describe an emerging package of technologies, [secure access service edge](#) (SASE) combines a software-defined wide area network (SD-WAN) with network security services into a single, cloud-delivered service.

In a modern enterprise network, application awareness, integrated SASE and SD-WAN are peanut butter, jam and bread because they complement each other's strengths, creating what is quickly proving to be robust, secure and efficient network infrastructures. What company doesn't want that?

The biggest difficulty has been that for decades, enterprises have been buying so-called "best-of-breed" point products for each part of the network security apparatus, and those are difficult to maintain and fix over time on an individual basis. Each piece of the network is intricately

connected and dependent upon each other piece, often taking a great deal of staff time and work to make adjustments. Throw in a bevy of different vendors, and you're probably working every night and weekend.

This is why platform solutions, which have none of these issues, are the clear trend – in all sectors of IT – in 2023.

The "better together" approach has been a long-standing theme at Palo Alto Networks, rather than a recent development. Over time, Prisma SD-WAN has improved its integration and consolidation, making it easier to bring every aspect of data access into the solution and vice versa. This allows for a common policy configuration across both solutions.

As IT moves into its inevitable new phases from year to year, replacing older tech that worked well in its day but has been supplanted by faster, more efficient apps and platforms, legacy networking products are fast becoming obsolete. Network administrators no longer need to maintain and patch a dozen or more products running 24/7 and know the ins and outs of every piece of legacy software or hardware.

When combined in the same platform, application awareness, SD-WAN and SASE offer the following advantages:



**Simplified management:** Integrating these elements allows for centralized management and orchestration of both security and network functions, which simplifies administration and reduces operational complexity.



**Improved performance:** SD-WAN optimizes application performance and network traffic by intelligently routing data across multiple WAN links. Application awareness greases these skids. With tight integration with SASE, SD-WAN can connect to the closest proximity security services in a cloud-delivered model to provide low latency connections to all apps.



**Automated Day 2 operations:** SD-WAN with native integration to Autonomous Digital Experience Management (ADEM) can deliver detection and predictive analytics to remediate issues proactively. Additionally, ADEM delivers always-on observability to empower IT to stay up to date on their end-to-end network health.

---

## In Summary

With application awareness, SASE and SD-WAN components are tuned to work collaboratively in an IT system, it creates a multifaceted, flexible and cost-effective package that addresses all networking and security challenges faced by enterprises. This synergy has been shown to provide improved performance, better-organized security and more effective time management. What network administrator doesn't want this?

The challenge now is for C-level IT leaders to realize the long-term benefits of using such a platform data management system to run an enterprise network.

Learn more about how the application awareness of [Prisma SD-WAN](#) can deliver an unmatched user experience



### About Prisma SD-WAN

Palo Alto Networks Prisma SASE powers the branch of the future that is hybrid, digitized and secure with next-generation SD-WAN. Unlike the Gen-1 SD-WAN solution, it provides flexible and resilient connectivity on any WAN and application SLAs. Furthermore, it provides Zero Trust security for users, apps and IoT devices, and automates Day 2 operations with AIOps. As a result, businesses can seamlessly deliver exceptional user experience, secure their network holistically (incl IoT), and simplify complex IT operations.

[www.paloaltonetworks.com/sase/sd-wan](http://www.paloaltonetworks.com/sase/sd-wan)



### About SDxCentral

SDxCentral is a B2B media and martech company. On the media side, we leverage our expertise to empower IT professionals to make better decisions for their organizations while advancing their careers. Our content educates and informs cloud, networking, and security professionals working in operations, development, and leadership within large enterprises and service providers. On the martech side we use buyer engagements to understand and predict intent, connecting our clients with engaged IT professionals. Combined with data-driven custom content, our martech solutions enable industry professionals from corporate marketing to product marketing and sales to influence IT buyers and turn them into customers.

[www.sdxcentral.com](http://www.sdxcentral.com)

---